

CLAIMS

Now, therefore, the following is claimed:

- 1 1. A system for securely transmitting data messages, comprising:
- 2 a first computer configured transmit a data message, said data
- 3 message having a header and a data portion, said first computer
- 4 configured to encrypt said data portion via a first encryption
- 5 technique and to encrypt said header via a second encryption
- 6 technique, said first computer further configured to include
- 7 information associated with said first encryption technique in said
- 8 header; and
- 9 a second computer configured to receive said first data message
- 10 and to decrypt said header, said second computer further configured
- 11 to decrypt said data portion based on said information included in
- 12 said header.
- 1 2. The system of claim 1, wherein said information associated with said first
- 2 encryption technique identifies said second encryption technique.
- 1 3. The system of claim 1, wherein said second encryption technique includes
- 2 RSA encryption.

1 4. The system of claim 3, wherein said first encryption technique includes
2 DES encryption.

a! 1 5. The system of claim 1, wherein said first computer transmits a public key
2 to said second computer, and wherein said second computer utilizes said public key
3 to decrypt said header.

1 6. The system of claim 5, wherein said first computer is configured to
2 encrypt said public key before transmitting said public key to said second computer.

1 7. The system of claim 1, wherein said information associated with said first
2 encryption technique identifies an encryption key used by said first computer to
3 encrypt said data portion.

1 8. The system of claim 7, wherein said first computer randomly selects said
2 encryption key.

1 9. The system of claim 1, wherein said second computer is configured to
2 transmit a list of encryption techniques to said first computer and said first
3 computer is configured to select said first encryption technique from said list.

1 10. The system of claim 9, wherein said first computer randomly selects said
2 first encryption technique from said list.

1 11. A system for transmitting messages, comprising:
2 means for defining a data portion of a data message;
3 means for encrypting said data portion via a first encryption technique;
4 means for defining a header of said data message, said header including
5 information associated with said first encryption technique;
6 means for encrypting said header via a second encryption technique; and
7 means for transmitting said message.

1 12. A method for transmitting messages, comprising the steps of:
2 defining a data portion of a first data message;
3 encrypting said data portion of said first data message via a first
4 encryption technique;
5 defining a header of said first data message, said header of said first data
6 message including information associated with said first encryption
7 technique;
8 encrypting said header of said first data message via a second encryption
9 technique; and
10 transmitting said first data message subsequent to said encrypting steps.

1 13. The method of claim 12, further comprising the steps of:

2 receiving a list of encryption techniques; and

3 randomly selecting said first encryption technique from said list.

a 1 14. The method of claim 12, wherein said first encryption technique includes RSA
2 encryption.

1 15. The method of claim 14, wherein said second encryption technique includes DES
2 encryption.

1 16. The method of claim 12, wherein said encrypting said data portion step includes
2 the step of encrypting said data portion of said first data message with an
3 encryption key, said method further comprising the step of including said
4 encryption key in said header of said first data message.

1 17. The method of claim 16, further comprising the step of randomly selecting said
2 encryption key.

1 18. The method of claim 12, further comprising the steps of:
 2 receiving said first data message transmitted in said transmitting step;
 3 decrypting said header of said first data message; and
 4 decrypting said data portion of said first data message based on said
 5 information included in said header of said first data message.

1 19. The method of claim 18, further comprising the step of identifying said first
 2 encryption technique via information included in said header of said first data
 3 message.

1 20. The method of claim 18, further comprising the steps of:
 2 transmitting a public key; and
 3 decrypting said header of said first data message based on said public key.

1 21. The method of claim 20, further comprising the step of encrypting said public key
 2 before said transmitting a public key step.

1 22. The method of claim 12, further comprising the steps of:
 2 defining a data portion of a second data message;
 3 encrypting said data portion of said second data message via a third
 4 encryption technique;
 5 defining a header of said second data message, said header of said second
 6 data message including information associated with said third
 7 encryption technique;
 8 encrypting said header of said second data message via said second
 9 encryption technique; and
 10 transmitting said second data message.

1 23. The method of claim 22, further comprising the step of randomly selecting said
 2 first and third encryption techniques.

1 24. The method of claim 23, further comprising the steps of:
 2 receiving said second message;
 3 decrypting said header of said second message; and
 4 decrypting said data portion of said second message based on said
 5 information included in said header of said second message.